(9) CLAIMS

1. A method for predicting potential points-of-compromise, the method comprising:

storing a database correlating each first member of a first set, wherein each of said first members may be compromised in time, with each second member of a second set, wherein each of said second members may be a potential point-of compromise;

recording in said database each interaction of a first member with a second member;

from a given third set of third members, wherein each of said third members is a given compromised first member, from said database, selecting each interaction associating said third members and said second members;

calculating an interaction factor for each of said third members from each said interaction; and

predicting at least one potential point-of-compromise from results of said calculating.

2. The method as set forth in claim 1 said selecting further comprising:

for each of said third members, including each said interaction found for a predetermined past time period.

3. The method as set forth in claim 2 wherein each said predetermined

past time period is determined individually from a given time-of-first-know-fraud for each of said third members.

4. The method as set forth in claim 3 wherein said storing and said recording further comprises:

dividing said database into a plurality of separately retrievable files wherein each of said files is characterized by a predetermined time frame bounding interactions between said first members and said second members.

5. The method as set forth in claim 4 wherein for each of said third members said each said time-of-first-known-fraud and said predetermined time frame is used to filter out those separately retrievable files not within said predetermined past time period from said selecting.

6. The method as set forth in claim 4 wherein said separately retrievable files are created using identifier features of said second members suited to maximizing data compression.

7. The method as set forth in claim 1, said storing further comprising:

segregating correlated first members and second members into a plurality of data files wherein said files are identifiable via a predetermined common characteristic of at least one predetermined particular characteristic of a selected on of said first members or said second members.

8. The method as set forth in claim 7 wherein said segregating further comprises:

creating two-hundred-fifty-six files.

9. The method as set forth in claim 1, said predicting further comprising:

listing all second members associated in said selecting as a potential point-of-compromise with a score based upon a tally of interactions between said third members and said second members.

10. The method as set forth in claim 9, said predicting further comprising:

adjusting each said score by a common factor associated with each said second member associated in said selecting wherein all scores are normalized.

11. A method for identifying possible points-of-compromise, the method comprising:

creating a matrix correlating a plurality of at least two identifiers;

logging in said matrix every interactivity involving individual ones of each of said two identifiers;

from a given set of first specific identifiers, extracting from said matrix all interactivities with second identifiers for said set;

tabulating extracted said interactivities according to frequency of said interactivities; and

assigning a point-of-compromise score to each of said first identifiers wherein each said score is indicative of frequency of the extracted interactivities.

12. The method as set forth in claim 11 further comprising:

sorting said matrix into a plurality of data files such that in each of said files one of said identifiers has a predetermined unique characteristic; and

using a given identifier having said characteristic, retrieving from one of said files associated with said characteristic, each second identifier from said matrix having at least one of said interactivities.

13. The method as set forth in claim 11 further comprising:

limiting said extracting to a predetermined past time frame.

14. The method as set forth in claim 12 wherein each of said files is associated with a common structure or characteristic of at least one of said identifiers.

15. The method as set forth in claim 11 wherein each said interactivity is a data pair further comprising a fixed first identifier representative of a compromised identifier and an interactivity situation identifier.

16. The method as set forth in claim 15 wherein one particular interactivity

identifier comprises one or more potential point-of-compromise identifiers.

17. A data storage and data mining process for determining at least one probable point-of-compromise for members of a data set, the process comprising:

in a set of data files, logging every individual transaction between first members and second members, wherein said first members are subject to compromise and said second members are each a potential point-of-compromise;

from a given set of compromised first members, segregating a subset of the data files for a predetermined time period past wherein said subset has at least one of said first members logged therein;

for each of said second members in said subset, incrementing a separate second member tally for each said individual transaction associated with each one of said compromised first members, creating a set of tallies associated with each of said second members; and

organizing said set of tallies according to a predetermined scoring statistic associated with probability of point-of-compromise.

18. A data storage and data mining system for determining at least one probable point-of-compromise for members of a data set, the system comprising:

means for storing data files;

means for logging in said data files every individual transaction between first members and second members, wherein said first members are subject to compromise and said second members are each a potential point-of-compromise;

from a given set of compromised first members, means for segregating a subset of the data files for a predetermined time period past wherein said subset has at least one of said first members logged therein;

for each of said second members in said subset, means for incrementing a separate second member tally for each said individual transaction associated with each one of said compromised first members and for creating a set of tallies associated with each of said second members; and

means for organizing said set of tallies according to a predetermined scoring statistic associated with potential as a point-of-compromise.

19. A method of determining credit card fraud point-of-compromise scores, the method comprising:

correlating all issued credit cards with all authorized points-of-use such that every transaction involving use of a credit card is retrievably logged in a database;

from a given set of compromised credit cards, extracting from said database all transactions involving use of each of said compromised credit cards;

for each of said authorized points-of-use involved in at least one of

said transactions involving at least one of said compromised credit card, creating a tally of said transactions for each point-of-use, incrementing each said tally for each occurrence of transaction involving at least one of said compromised credit cards;

sorting said authorized points-of-use having a tally according to tally score; and

assigning a score representative of point-of-compromise likelihood to each of said authorized points-of-use having a tally according to said tally score.

20. The method as set forth in claim 19 wherein said extracting is limited to a predetermined time period range of past transactions.

21. The method as set forth in claim 19 wherein each said tally score is normalized via a characteristic related to point-of-use .

22. The method as set forth in claim 19 wherein said database comprises a plurality of files wherein each of said files is characterized by a given time frame bounding said transactions logged.

23. The method as set forth in claim 22 wherein each of said plurality of files is sortable by identifier data representative of subsets of credit card numbers.

24. The method as set forth in claim 23 wherein said plurality of files includes 256 or 256^n files sorted by said identifier data.

25. The method as set forth in claim 20 wherein said predetermined time period range of past transactions is based upon a given suspected time-of-compromise window prior to a time-of-first-known-fraud for each said credit card.

26. The method as set forth in claim 22 wherein said files comprise a matrix of data compressed identifier pairs wherein each of said pairs includes a credit card identifier and a point-of-use situation identifier.

27. The method as set forth in claim 26 wherein a first database comprises a relational data pair relating said point-of-use situation identifier and said credit card identifier and a second database correlating each said point-of-use situation identifier to a physical said point-of-use.

28. A method of doing business comprising:

receiving a set of credit card numbers and a set of merchants authorized to accept said credit cards;

forming a matrix of said numbers and said merchants;

logging each use of a card with a merchant as a predetermined data point of said matrix;

from a given set of compromised credit card numbers, extracting therefor over a predetermined given time period, each related said data point of said matrix;

incrementing a tally for each merchant associated with each related said data point;

sorting said merchants by tally score; and

assigning a probability of point-of-compromise for said list of compromised credit card numbers based on said tally score.

29. A computer memory comprising:

computer code for compiling a database wherein members of a first class are associated with members of a second class in accordance with each interaction of a member of the first class with a member of the second class;

computer code for extracting from said database only those interactions for a predetermined past time period associated with a given subset of members of the first class wherein said given subset represents individual compromised members of said first class; and

computer code for assigning a score to individual members of the second class for each of said interactions extracted wherein said score represents a point-of-compromise probability for each of said individual members of the second class.

30. Given a computerized matrix of interactivity events between items-of-use, each having a unique first identifier, and points-of-use, each having a unique second identifier, and a set of compromised said items-of-use, wherein said matrix further comprises a plurality of files, each of said files covering a given time frame for said interactivity events, a method for point-of-compromise scoring comprising:

determining a time-of-first-known-fraud for each said compromised said items-of-use;

for each said compromised said items-of-use, assigning a suspected date window prior to said time-of-first-known-fraud;

selecting those ones of said files included in said suspected date window wherein said compromised said items-of-use are included in said files;

for each selected file and for each compromised said items-of-use, counting the number of said interactivity events for each of said points-of-use in each said selected file; and

assigning the highest score indicative of point-of-compromise to a highest scoring one of said points-of-use.